The Connectivity and Fault-Tolerance of the Internet Topology*

Christopher R. Palmer
Computer Science Department,
Carnegie Mellon University
Pittsburgh, PA 15213

Georgos Siganos
U.C. Riverside,
Dept. of Comp. Science
Riverside, CA 92521

Michalis Faloutsos
U.C. Riverside,
Dept. of Comp. Science
Riverside, CA 92521

Christos Faloutsos
Computer Science Department,
Carnegie Mellon University
Pittsburgh, PA 15213

Phillip B. Gibbons
Information Sciences Research Center,
Bell Laboratories
Murray Hill, NJ

Abstract

In this paper, we apply data mining analysis to study the topology of the Internet, thus creating a new processing framework. To the best of our knowledge, this is one of the first studies that focus on the Internet topology at the router level, i.e., each node is a router. The size (280K nodes) and the nature of the graph are such that new analysis methods have to be employed. First, we suggest computationally-expensive metrics to characterize topological properties. Then, we present an efficient approximation algorithm that makes the calculation of these metrics possible. Finally, we demonstrate the initial results of our framework. For example, we show that we can identify "central" routers, and poorly connected or even isolated nodes. We also find that the Internet is surprisingly resilient to random link and router failures, having only small changes in the connectivity for fewer than 10,000 failures. Our framework seems a promising step towards understanding and characterizing the Internet topology and possible other real communication graphs such as web-graphs.

1 Introduction

In this paper, we study the topology of the Internet at the router level. We know very little about the Internet, despite the significance and impact of the network in everyday life. This is especially true for the topology of the network, which is a crucial part of modeling and simulating the network. First, we study the structure of the network. Using topological properties, we manage to identify "different" parts of the network such as central backbone routers and areas with poor connectivity. Second, we study the robustness of the topology to edge and node failures. In our study, we use a novel data mining tool to process the large topological data.

* This material is based upon work supported by the National Science Foundation under Grants No. 9985195, IIS-9910606, LIS-9720374, by the Defense Advanced Research Projects Agency under Contract No. N66001-97-C-8517 and award N660001-00-1-8936, Dimi matching fund DIM00-10071 and by the Sun Educational Fellowship. Any opinions, findings, and conclusions or recommendations expressed in this material are those of the author(s) and do not necessarily reflect the views of the National Science Foundation, DARPA, or other funding parties.

Why can't we model the Internet topology? There are several reasons for that. First, the necessary data has only recently become available. Second, the data is so large (285K nodes) that standard processing and visualization techniques are inadequate. Despite these challenges, it is very important to characterize the topology. The absence of this knowledge is one of the reasons "Why we don't know how to simulate the Internet" according to Paxson and Floyd [11]. It is very difficult to analyze and optimize network performance without understanding its topology. It is analogous to resolving traffic problems in a city without a map.

The novelty of our work lies in the use of data mining tools in the study of the network topology. In more detail, we use a new tool to approximate the size of the neighbourhood of a node. This is a computationally expensive procedure and it is made feasible by our tool that reduces its run-time by more than a factor of 400. Given this tool, we are able to provide results in two main directions. First, we provide new insight in the structure of the graph, and we classify nodes according to their neighbourhood related properties. For example, we show that by using our analysis framework, we can distinguish nodes which may correspond to centrally-located or backbone routers. Second, we study the robustness of the network to edge and node failures. We find that the network is robust to edge failures, and uniformly distributed node failures. However, we observe that failures in the central or backbone nodes can very quickly hurt the connectivity of the network. In our work, we use some of the novel graph metrics proposed by Faloutsos et al [4] and we show that these metrics can actually provide insight into the graph structure.

In section 2 we present the background, summarize previous work and define our novel Internet metrics. In section 3, we highlight the approximation algorithm that we use. In section 4, we present our results. Finally in section 5, we present our conclusions.

2 Background/Novel Graph Metrics

We begin this section by defining the terminology that we will use in the remainder of the paper. We also describe the Internet router data that we will be using.

We study the network at the *router level*, that is, each Internet router is represented by a node in the graph while each link is mapped by an edge. In contrast, a lot of previous work has concentrated on the interdomain level of the topology where each graph node represents a domain or Autonomous System. The router level is a much larger and more detailed graph. We believe that the size of this graph has made its processing prohibitively expensive.

We list a number of graph metrics that have been proposed in the literature only recently. Typical metrics are average node degree and diameter. We believe that the *hop exponent*, *effective diameter* and *effective eccentricity* are much more effective in characterizing the complexity of the Internet graph.

Definitions. Let $G = (V, E)$ be either a directed or undirected graph. Let $d(u, v)$ be the shortest path distance from node u to node v. Define the following :

Reachable set: Nodes that are within distance h of u: $S(u, h) = \{v : d(u, v) \leq h\}$.

Individual neighbourhood function: Reachable sets sizes: $N(u, h) = |S(u, h)|$.

Neighbourhood function: Number of pairs of nodes within distance h: $N(h) = \sum_{u \in V} N(u, h)$.

Reachable pairs: Number of pairs of nodes that have a path connecting them: $N(\infty)$.

Effective diameter: Least distance, h, such that at least 90% of the reachable pairs are within distance h: $\min_h N(h) \geq .9 \cdot N(\infty)$

Effective eccentricity: Eccentricity is to a node as the diameter is to a graph. Least distance, h, such that 90% of u's reachable set are within distance h: $\min_h N(u, h) \geq .9 \cdot N(u, \infty)$.

Hop-plot exponent: A proposed power-law in [4], that the total number of pairs of nodes within h hops is proportional to the number of hops raised to a constant, $\mathcal{H}$ (*hop-plot exponent*).

We use the hop-plot exponent to characterize the growth of the neighbourhood function. To compute it, we apply log transforms to the neighbourhood function and compute the least-square fitting line for the points up to the effective diameter.

Our real Internet graph. We use the graph that is the result of the union of the SCAN [14] and Lucent Internet mapping project results [13]. The SCAN project developed a topology discovery tool called Mercator that uses hop-limited probes – the same primitive used in traceroute – to infer the map of the Internet [14]. The Lucent Internet mapping project uses a single probe location but has performed long term monitoring [8]. This merged data set represents the best map of the Internet (at a router level) which was current as of late 1999. The resulting graph has approximately 285K nodes, 430K edges, a maximum degree of 1,978 and an average degree of 3.15. It is this graph that we will use to study the router-level Internet topology.

Previous work. The neighbourhood of a node is important for estimating the complexity of various networking protocols such as DVMPR and QoSMIC [3, 16]. There have been several measurements of the Internet topology [6, 10, 7]. These studies focus on the collection of data while the analysis appears secondary. There has not yet been a comprehensive study of the Internet topology at the router level. In contrast, the interdomain level has been studied lately [15]. In a parallel tangent, several people have studied topological properties indirectly, through the study of scaling of multicast trees in Internet [2, 12, 17]. Recently, Albert et al [1] and Tauro and Faloutsos [15] studied the fault tolerance of the Internet at the interdomain level. Recall that our work here focuses at the router level of the Internet.

Assumptions and limitations. The router-level Internet graph contains communication links discovered over an extended period of time. As such, it may include alternative paths that were specifically created to remedy some network failures. We believe that our results show fundamental graph properties and not artifacts of the data collection process. Similarly, since our work relies on measured data, there is always some measurement error. The main problems with Internet measurements are a) incompleteness, b) router identification. We can not claim or guarantee that it is most of it, but we have reasons to believe that this data contains a substantial and representative part of the Internet. For a discussion on this issue see [14, 7, 8].

3 Approximate Neighbourhood Function (ANF)

We have developed and evaluated an approximate neighbourhood function (ANF) in [9]. We present the key ideas and a simple version of the algorithm. The algorithm is presented in sufficient detail to reproduce the results in this paper. The underlying approach is to iteratively compute $S(u, h)$, the set of nodes within at most h hops of u, using the edge set and $S(u, h-1)$. That is:

```
FOR each node u DO S(u,0) = { u }
FOR each iteration, h starting at 1
   FOR each node u DO S(u,h) = S(u,h-1)
   FOR each edge (u,v)
      DO S(v,h) = S(v,h) U S(u,h-1)
```

and then the neighbourhood function is

```
FOR each node, u DO
   M(u,0) = concatenation of k bitmasks, each with 1 bit set
            (according to an exponential distribution)

FOR each distance, it, starting with 1 DO
    FOR each node, u DO M(u,it) = M(u,it-1)
    FOR each edge (u,v) DO M(u,it) = (M(u,it) OR M(v,it-1))
    The estimate is: SUM(all u) (2^b)/(.7731*bias)
        where b is the average of the least zero bits in the k bitmasks
              bias, a small bias factor, is (1+.31/k)
```

Figure 1: In-Core Approximate Neighbourhood Function (ANF)

$$N(h) = \sum_u |S(u,h)|.$$

This algorithm will be horribly inefficient to use in practice because the set operations are expensive. Instead, we use a tool called approximate counting. An *approximate counting* algorithm takes as input a multi-set and then estimates the number of distinct elements in the multi-set. In [5], each possible element (for us, that is each node) is assigned a random bit using an exponential distribution (half the nodes get bit 0, a quarter get bit 1, etc.). To estimate the number of elements in a multi-set, you simply `OR` together the bits that we assigned to each element. The estimate is then close to 2^b, where b is the least zero bit in the bitmask. We can use the approximate counting idea to replace the set operations in our simple algorithm. We use $M(u,h)$ to denote the bitmask approximation to $|S(u,h)|$ and to improve accuracy perform the approximation k times in parallel (we fix $k = 64$ for the remainder of the paper). This algorithm appears in Figure 1 and operates only in-core. An external version of the algorithm is also presented in [9] which allows the processing of graphs that are much larger than available memory.

The ANF algorithm has several properties that make it possible to perform studies on large graphs. Here we will just list its properties, while [9] looks in detail at its efficiency and the quality of estimation.

- **Fast:** Approximate the neighbourhood function of the router level graph (285K nodes and 430K edges) in a matter of minutes, rather than nearly a day (436x faster).
- **Accurate:** The approximates have provable bounds, generally within 5-10% of the true function for our experiments.
- **Individual neighbourhood functions:** As a by-product of computing the neighbourhood functions, we compute the neighbourhood function for each individual node.

4 Data-Mining the Internet Graph

In this section, we show how the new approximation algorithm enables us to find interesting properties of the Internet topology. First, we study the structure of the network by identifying properties of the nodes. Second, we study the robustness of the topology to component failures.

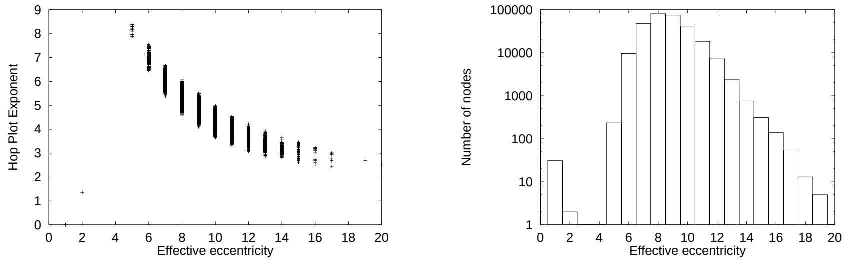
4.1 Discovering Structure Through Node Classification

The first application of the neighbourhood function is to examine the individual routers in the Internet graph. We wish to understand the connectivity richness of different routers. Note that this corresponds loosely to alternate paths that the node could potentially use. That is, we know that the effective diameter of the Internet is approximately 10 hops, but how does that translate to the path lengths for individual nodes?

Quantifying the relationship of hopplot and eccentricity. We conducted an experiment with results in Figure 2 a). First we compute the individual neighbourhood functions for all nodes in the graph. From this, we measure the effective eccentricity of each node and compute the hop exponent for each individual neighbourhood function. The scatter plot of these values indicates a strong correlation between the eccentricity and the hop exponent (not surprising).

Classifying nodes using eccentricity. In Figure 2 b), we show the histogram of the number of nodes with each effective eccentricity. The number of nodes is plotted in log scale. We observe that about 10,000 routers have an effective eccentricity of at most 6 and another 10,000 routers have an effective eccentricity of 12 or larger. The majority of the nodes have an effective eccentricity that is close to the effective diameter of the Internet.

Identifying pathologies of the measured data. Our analysis can help identify pathological or incomplete cases in the measured data. We observe that there are some nodes with eccentricity 1 and 2. This would mean that a node has a degree of approximately



a) Hop exponent vs. Effective diameter b) Histogram of diameters

Figure 2: Hop exponent and effective eccentricities of the individual neighbourhood functions for Internet routers

$0.9 \cdot 284\text{K} = 250\text{K}$ links. This is clearly not the case, since the max degree of the graph is no more than 2K. The explanation is that the graph has some disconnected components. Recall that we define the eccentricity relative to the nodes that *can be* reached. For example, an isolated pair of nodes has eccentricity 1. We checked the data in the graph and found that this was actually the case for the nodes reported here.

4.2 Topological Fault-tolerance

When looking at the failure behaviour of a network, there are two contributing factors. First, network outages may disconnect pairs of nodes. Second, protocol failures may cause pairs of nodes to appear disconnected even though a physical path exists between them. In this section, we explore the first form of failure. Network outages may involve a physical link between a pair of routers being lost (for example, as a result of a backhoe breaking a network cable) or may involve a computer failing completely. We are not considering the effects of routing policies or algorithms. It is important to understand what communication patterns are physically possible before attempting to understand what communication is possible given a specific protocol or policy.

4.2.1 Link Failures

We want to examine the robustness of the Internet with respect to link failures. Thus, we conduct the following experiment. We select x edges at random and delete them. We then approximate the neighbourhood function, the effective diameter, the number of reachable pairs and the hop exponent using the ANF algorithm.

The Internet is robust to link failures. The number of reachable pairs, and the hop exponent shown as a function of the number of edge deletions appears in Figure 3. Each point is the average over 3 randomly chosen sets of edges. We have not shown the average diameter as it only varies from 10 to approximately 12 over the full set of edge deletions. This shows that while we delete edges, pairs of nodes either become disconnected or they have an alternative path that is not significantly longer. We see that the Internet is quite resilient under connection failures, with only a small decrease in the number of reachable pairs and the hop exponent for fewer than 50,000 failures. Moreover, deleting edges does not appear to change the hop exponent until closer to 200,000 deletions, suggesting that while we partition the Internet, the structure is preserved.

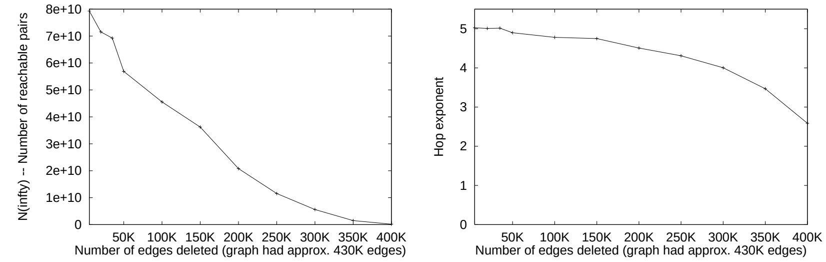
4.2.2 Node Failures

Router failures represent a more catastrophic event, since a router affects all its adjacent edges. Therefore, we expect that this will cause problems at least in the vicinity of the node. To model a router failure, we select a node (in one of three different ways) and delete all its adjacent edges.

We introduce failures in three different ways. First, we randomly select routers (uniform distribution). This corresponds to an unbiased router-specific failure. Second, we take the opposite of the previous approach. We remove the nodes in order of highest degree. This is the most aggressive approach that we can take to decompose the Internet. The final method that we use removes nodes in order of highest individual hop exponent. We theorized in section 4.1 that the nodes with low effective diameter and high hop exponent may be important nodes, possibly in the backbone.

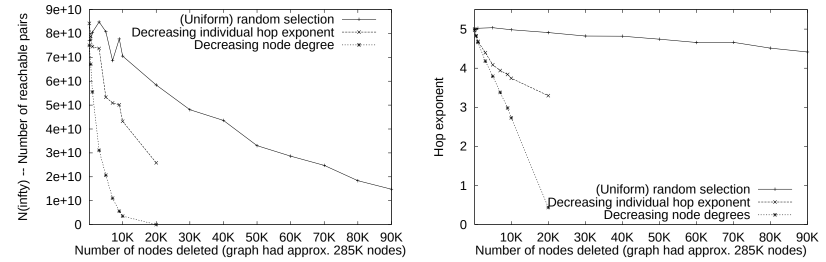
For each of the different node selection methods, above, we approximate the neighbourhood function, the effective diameter, the number of reachable pairs and the hop exponent using the ANF algorithm. These results are shown in Figure 4.

The Internet is robust to random node failures. Here we see that fewer than about 10,000 router failures does not significantly affect the Internet. That is, the number of reachable pairs is not drastically reduced. Moreover, the hop exponent is not decreasing very quickly with the number of deleted nodes. This suggests that it might be possible to use sampled Inter-



a) Nodes that can communicate b) Change in hop exponent

Figure 3: Effect of edge deletions (connection failures) on the router graph



a) Nodes that can communicate b) Change in hop exponent

Figure 4: Effect of node deletions (router failures) on the router graph

net graphs to conduct reliable simulation experiments.

The Internet is sensitive to focused failures. The other two approaches for router selection have much more devastating results. By selecting routers according to their degree, we can quickly disconnect the Internet. Only 10,000 nodes are needed to effectively disconnect most node pairs. Even 100 of these nodes is sufficient to remove the connectivity in more than 5 billion pairs.

The effective eccentricity as a node classifier. The above observation confirms that the effective eccentricity is a useful graph metric. Nodes with high eccentricity are "important" for the network; their failures create problems to the connectivity of the network. At the same time, we see that eccentricity has a different effect than the degree regarding the connectivity. This observation suggests that eccentricity quantifies another aspect of the "importance" of the node and it is distinct from the node degree.

5 Conclusions

In this paper we proposed a set of new and existing metrics that capture interesting topological properties of the Internet. While these metrics are expensive to compute exactly, we have shown that a new data mining tool can be very effective in approximating these metrics. This has allowed us to obtain new insights into the properties of routers and their "importance" for the network. Further use of these ideas allowed us to examine the intrinsic resilience of the Internet.

Our work highlights the untapped potential that exists for the use of data-mining tools in network data; the size of the network makes classic techniques prohibitively expensive in computation time. In more detail our results can be summarized in the following points:

- We propose a new set of new and existing metrics capturing interesting topological properties.
- We show that a new data mining tool can be very effective in calculating the otherwise computationally expensive metrics.
- Effective eccentricity is a good node metric, for the "topological significance" of a node and it captures a different aspect than that of the node degree.
- The Internet topology is resilient to random link and node failures.
- The Internet is sensitive to focussed node failures; it is sensitive to failures of high "significance" nodes, expressed either by its degree or effective eccentricity.

Our metrics and tool make a promising step towards understanding and characterizing the Internet topology and possible other real communication graphs such as web-graphs. We are in the process of developing more methods to decipher the structure of the Internet topology. Our initial results are encouraging.

References

[1] R. Albert, H. Jeong, and A. Barabasi. Attack and error tolerance of complex networks. *Nature*, 406, July 2000.

[2] J. Chuang and M. Sirbu. Pricing multicast communications: A cost based approach. *In Proc. of the INET'98*, 1998.

[3] M. Faloutsos, A. Banerjea, and R. Pankaj. QoSMIC: a QoS Multicast Internet protoCol. *ACM SIGCOMM*, September 2-4, Vancouver BC 1998.

[4] M. Faloutsos, P. Faloutsos, and C. Faloutsos. On power-law relationships of the internet topology. In *SIGCOMM*, 1999.

[5] P. Flajolet and G. N. Martin. Probabilistic counting algorithms for data base applications. *Journal of Computer and System Sciences*, 31:182–209, 1985.

[6] R. Govindan and A. Reddy. An analysis of internet inter-domain topology and route stability. *Proc. IEEE INFOCOM*, Kobe, Japan, April 7-11 1997.

[7] R. Govindan and H. Tangmunarunkit. Heuristics for internet map discovery. *Proc. IEEE INFOCOM*, Tel Aviv, Israel, March 2000.

[8] Internet mapping project. `http://cm.bell-labs.com/who/ches/map/index.html`.

[9] C. R. Palmer, P. B. Gibbons, and C. Faloutsos. A fast approximation of the "neighbourhood" function for massive graphs. Technical Report CMU-CS-01-122, Carnegie Mellon University, 2001.

[10] J.-J. Pansiot and D. Grad. On routes and multicast trees in the Internet. *ACM Computer Communication Review*, 28(1):41–50, January 1998.

[11] V. Paxson and S. Floyd. Why we don't know how to simulate the internet. *Proceedings of the 1997 Winter Simulation Conference*, December 1997.

[12] G. Philips, S. Shenker, and H. Tangmunarunkit. Scaling of multicast trees: Comments on the Chuang-Sirbu scaling law. *ACM SIGCOMM*, September 1999.

[13] SCAN project. `http://www.isi.edu/scan/mercator/maps.html`.

[14] SCAN project proposal. `http://www.isi.edu/scan/Pubs/scan_proposal.ps.gz`.

[15] S.L. Tauro and M. Faloutsos. Fault-tolerance and robustness of the internet topology. *PRDC 2000, (abstract), Los Angeles*, 2000.

[16] D. Waitzman, C. Partridge, and S. Deering. Distance vector multicast routing protocol. IETF RFC 1075, 1998.

[17] T. Wong and R. Katz. An analysis of multicast forwarding state scalability. *International Conference on Network Protocols*, 2000.